


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

THE ACM DIGITAL LIBRARY
[Feedback](#)

(portable executable) and (portable and executable) and (worm or virus or trojan or malware or malicious)

Terms used:

Found 147 of 1

portable executable portable executable worm virus trojan malware malicious

 Sort results by
[Save results to a Binder](#)

Refine these results

 Display results
☐ [Open results in a new window](#)

 Try this search in [The](#)

Results 1 - 20 of 147

 Result page: 1 2 3 4 5 6 7 8 [next](#) [>>](#)

1 [Are handheld viruses a significant threat?](#)



Simon N. Foley, Robert Dumigan

January 2001 Communications of the ACM, Volume 44 Issue 1

Publisher: ACM

 Full text available: pdf(119.80 KB) html(17.24 KB) [Additional Information: full citation, references, index terms](#)

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 69, Citation Count: 0

2 [Attack of the killer virus!](#)



Dennis Fowler

December 2003 netWorker, Volume 7 Issue 4

Publisher: ACM

 Full text available: pdf(80.81 KB) html(22.25 KB) [Additional Information: full citation, abstract, index terms](#)

Bibliometrics: Downloads (6 Weeks): 16, Downloads (12 Months): 128, Citation Count: 0

Though more than 600 million people worldwide use the Internet, it takes only one virus writer to make just about all of us miserable. Like a single stray neutron in a critical mass of plutonium, a virus can trigger a chain reaction that spews thousands ...

3 [Learning to detect malicious executables in the wild](#)



Jeremy Z. Kolter, Marcus A. Maloof

August 2004 KDD '04: Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining

Publisher: ACM

 Full text available: pdf(216.52 KB) [Additional Information: full citation, abstract, references, cited by, index term](#)

Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 137, Citation Count: 3

In this paper, we describe the development of a fielded application for detecting malicious executables in the wild. We gathered 1971 benign and 1651 malicious executables and encoded each as a triple example using n-grams of byte codes as features. ...

Keywords: concept learning, data mining, malicious software, security

4 [Visualizing windows executable viruses using self-organizing maps](#)



InSeon Yoo

October 2004 VizSEC/ DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security

Publisher: ACM

Full text available: pdf(571.27 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index term](#)

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 62, Citation Count: 0

This paper concentrates on visualizing computer viruses without using virus specific signature information as a prior stage of the very important problem of detecting computer viruses. In this paper, we address the fact that each viruses have its own ...

Keywords: self-organizing maps, visualization, windows executable viruses

5 [Detection of injected, dynamically generated, and obfuscated malicious code](#)



Jesse C. Rabek, Roger I. Khazan, Scott M. Lewandowski, Robert K. Cunningham

October 2003 WORM '03: Proceedings of the 2003 ACM workshop on Rapid malware

Publisher: ACM

Full text available: pdf(240.68 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index term](#)

Bibliometrics: Downloads (6 Weeks): 14, Downloads (12 Months): 154, Citation Count: 5

This paper presents DOME, a host-based technique for detecting several general classes of malicious code in software executables. DOME uses static analysis to identify the locations (virtual addresses, system calls within the software executables, ...

Keywords: anomaly detection, code analysis, dynamic analysis, execution monitoring, intrusion detection, malicious code detection, static analysis, system calls

6 [Learning to Detect and Classify Malicious Executables in the Wild](#)

J. Zico Kolter, Marcus A. Maloof

December 2006 The Journal of Machine Learning Research, Volume 7

Publisher: MIT Press

Full text available: pdf(242.79 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index term](#)

Bibliometrics: Downloads (6 Weeks): 12, Downloads (12 Months): 166, Citation Count: 2

We describe the use of machine learning and data mining to detect and classify malicious executables as they appear in the wild. We gathered 1,971 benign and 1,651 malicious executables and encoded each as a training example using n -grams of byte ...

7 [Building an e-mail virus detection system for your network](#)

Dave Jones

December 2001 Linux Journal, Volume 2001 Issue 92

Publisher: Specialized Systems Consultants, Inc.

Full text available: html(22.15 KB)

Additional Information: [full citation](#), [abstract](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 56, Citation Count: 0

Jones gives a great example of a homegrown virus protection system.

8 A tool for analyzing and detecting malicious mobile code



Akira Mori, Tomonori Izumida, Toshimi Sawada, Tadashi Inoue

May 2006 I CSE '06: Proceedings of the 28th international conference on Software engineering

Publisher: ACM

Full text available: pdf(99.06 KB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 102, Citation Count: 0

We present a tool for analysis and detection of malicious mobile code such as computer viruses internet worms based on the combined use of code simulation, static code analysis, and OS exe emulation. Unlike traditional anti-virus methods, the ...

Keywords: OS execution emulation, code simulation, malicious code detection, static code anal

9 Static analysis of anomalies and security vulnerabilities in executable files



Jay-Evan J. Tevis, John A. Hamilton, Jr.

March 2006 ACM-SE 44: Proceedings of the 44th annual Southeast regional conference

Publisher: ACM

Full text available: pdf(119.85 KB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 83, Citation Count: 0

Software researchers have already developed static code security checkers to parse through and <u>source code</u> files, looking for security vulnerabilities [8, 9]. What about <u>executabl files</u> Can these files also ...

Keywords: PE format, executable file, software security vulnerabilities, static analysis

10 SPIKE: engineering malware analysis tools using unobtrusive binary instrumentation

Amit Vasudevan, Ramesh Yerraballi

January 2006 ACSC '06: Proceedings of the 29th Australasian Computer Science Conference

Volume 48, Volume 48

Publisher: Australian Computer Society, Inc.

Full text available: pdf(832.66 KB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 151, Citation Count: 0

Malware -- a generic term that encompasses viruses, trojans, spywares and other intrusive code widespread today. Malware analysis is a multi-step process providing insight into malware struc and functionality, facilitating the development of ...

Keywords: instrumentation, malware, security

11 IMDS: intelligent malware detection system



Yanfang Ye, Dingding Wang, Tao Li, Dongyi Ye

August 2007 KDD '07: Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining

Publisher: ACM

Full text available: pdf(1.22 MB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 39, Downloads (12 Months): 314, Citation Count: 0

The proliferation of malware has presented a serious threat to the security of computer systems Traditional signature-based anti-virus systems fail to detect polymorphic and new, previously ur malicious executables. In this paper, resting on the ...

Keywords: OOA mining, PE file, malware, windows API sequence

12 The reflective mobile agent paradigm implemented in a smart office environment

F. Bagci, H. Schick, J. Petzold, W. Trumler, T. Ungerer

October 2006 Personal and Ubiquitous Computing, Volume 11 Issue 1

Publisher: Springer-Verlag

Full text available:  pdf(308.96 KB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 14, Downloads (12 Months): 105, Citation Count: 0

Ubiquitous systems will integrate computers invisibly and unobtrusively in everyday objects. Data can be captured from single or multi-sensor devices and will be used for context extraction. New local-based services will be adapted to user preferences. ...

13 Eudaemon: involuntary and on-demand emulation against zero-day exploits

Georgios Portokalidis, Herbert Bos

April 2008 ACM SIGOPS Operating Systems Review, Volume 42 Issue 4

Publisher: ACM

Full text available:  pdf(381.70 KB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 0, Downloads (12 Months): 0, Citation Count: 0

Eudaemon is a technique that aims to blur the borders between protected and unprotected applications, and brings together honeypot technology and end-user intrusion detection and prevention. Eudaemon is able to attach to any running process, and redirect ...

Keywords: honeypots, operating systems, security

14 Using instruction block signatures to counter code injection attacks

Milena Milenković, Aleksandar Milenković, Emil Jovanov

March 2005 ACM SIGARCH Computer Architecture News, Volume 33 Issue 1

Publisher: ACM

Full text available:  pdf(283.67 KB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 47, Citation Count: 0

With more computing platforms connected to the Internet each day, computer system security has become a critical issue. One of the major security problems is execution of malicious injected code. In this paper we propose new processor extensions that ...

15 Review and analysis of synthetic diversity for breaking monocultures

James E. Just, Mark Cornwell

October 2004 WORM '04: Proceedings of the 2004 ACM workshop on Rapid malware

Publisher: ACM

Full text available:  pdf(356.14 KB)

Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 0, Downloads (12 Months): 39, Citation Count: 1

The increasing monoculture in operating systems and key applications and the enormous expense of N-version programming for custom applications mean that lack of diversity is a fundamental barrier to achieving survivability even for high value systems ...

Keywords: diversity, n-version programming, vulnerability

16 [Protecting C programs from attacks via invalid pointer dereferences](#)



Suan Hsi Yong, Susan Horwitz

September 2003 ACM SIGSOFT Software Engineering Notes, Volume 28 Issue 5

Publisher: ACM

Full text available: [pdf\(526.15 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 63, Citation Count: 10

Writes via unchecked pointer dereferences rank high among vulnerabilities most often exploited malicious code. The most common attacks use an unchecked string copy to cause a buffer over thereby overwriting the return address in the function's ...

Keywords: buffer overrun, instrumentation, security, static analysis

17 [A secure modular mobile agent system](#)



Adam Pridgen, Christine Julien

May 2006 SELMAS '06: Proceedings of the 2006 international workshop on Software engineering large-scale multi-agent systems

Publisher: ACM

Full text available: [pdf\(2.22 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 231, Citation Count: 0

Applications in mobile multi-agent systems require a high degree of confidence that code that runs inside the system will not be malicious and that any agents which are malicious can be identified contained. Since the inception of mobile agents, ...

Keywords: mobile agents

18 [Secure and practical defense against code-injection attacks using software dynamic translation](#)



Wei Hu, Jason Hiser, Dan Williams, Adrian Filipi, Jack W. Davidson, David Evans, John C. Knight, Ai Nguyen-Tuong, Jonathan Rowanhill

June 2006 VEE '06: Proceedings of the 2nd international conference on Virtual execution environments

Publisher: ACM

Full text available: [pdf\(270.13 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 154, Citation Count: 2

One of the most common forms of security attacks involves exploiting a vulnerability to inject malicious code into an executing application and then cause the injected code to be executed. A theoretically strong approach to defending against any type ...

Keywords: software dynamic translation, virtual execution

19 [VMM-based hidden process detection and identification using Lycosid](#)



Stephen T. Jones, Andrea C. Arpaci-Dusseau, Remzi H. Arpaci-Dusseau

March 2008 VEE '08: Proceedings of the fourth ACM SIGPLAN/SIGOPS international conference on Virtual execution environments

Publisher: ACM

Full text available: [pdf\(312.93 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)


Bibliometrics: Downloads (6 Weeks): 61, Downloads (12 Months): 61, Citation Count: 0

Use of stealth rootkit techniques to hide long-lived malicious processes is a current and alarming

security issue. In this paper, we describe, implement, and evaluate a novel VMM-based hidden process detection and identification service called Lycosid ...

Keywords: inference, security, virtual machine

20 Pallino: automation to support regression test selection for cots-based applications

 Jiang Zheng, Laurie Williams, Brian Robinson

November 2007 ASE '07: Proceedings of the twenty-second IEEE/ACM international conference on Automated software engineering

Publisher: ACM

Full text available:  pdf(233.61 KB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 37, Citation Count: 0

Software products are often built from commercial-off-the-shelf (COTS) components. When new releases of these components are made available for integration and testing, source code is usu not provided by the vendors. Various regression test selection ...

Keywords: COTS, commercial-off-the-shelf, regression testing, software testing

Results 1 - 20 of 147

Result page: 1 2 3 4 5 6 7 8 next >>

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  Adobe Acrobat  QuickTime  Windows Media Player  Real F